I claim:

1. A method of assuring that a message sent to a recipient was requested for opening by the recipient, the method comprising:

encrypting a message using a session key to produce an encrypted message;

encrypting the session key using a public key to produce an encrypted session key;

generating a transaction identifier;

encrypting the transaction identifier to provide an encrypted transaction identifier;

sending, by the sender, the encrypted session key and the transaction identifier to an arbiter;

sending, by the sender, the encrypted message and the encrypted transaction identifier to the recipient;

generating a request for the encrypted session key based on the transaction identifier;

sending the request to the arbiter; and

generating, by the arbiter, evidence that the request for the encrypted session key was received.

2. The method of claim 1 wherein the request comprises the transaction identifier and said generating evidence comprises logging that the transaction identifier was received.

3. The method of claim 1 wherein the request comprises the transaction identifier in unencrypted form such that the arbiter does not perform any cryptographic operations to extract the transaction identifier from the request.

4. The method of claim 1 wherein the arbiter does not receive the encrypted message delivered from the sender to the recipient.

5. The method of claim 1 further comprising notifying, by the arbiter, the sender of the request.

6. The method of claim 5 wherein said notifying comprises sending an e-mail to the sender.

7. The method of claim 1 wherein the request is repeatedly transmitted for a predetermined period of time by the recipient until the encrypted session key is received.

8. The method of claim 1, further comprising:

signing the decrypted transaction identifier, wherein said transmitting the request comprises sending the signed decrypted transaction identifier to the arbiter.

9. The method of claim 1 wherein said generating the request comprises:

decrypting, using the recipient's private key, the transaction identifier from the encrypted transaction identifier to provide a decrypted transaction identifier;

signing the decrypted transaction identifier and a nonce associated with that recipient; and

sending the signed decrypted transaction identifier and the nonce to the arbiter.

10. A system to assure that a message was requested for opening, comprising:

a sender to send encrypted decoding information and an encrypted message;

an arbiter to store the encrypted decoding information; and

a recipient to receive the encrypted message, request the encrypted decoding information, decrypt the encrypted decoding information and decrypt the encrypted message using the decrypted decoding information;

wherein the arbiter, in response to receiving the request, generates evidence that the request was received.

11. The system of claim 10 wherein the sender also sends a transaction identifier to the arbiter, the sender also sending an encrypted transaction identifier to the recipient, the transaction identifier being associated with the encrypted decoding information, the arbiter

storing the associated transaction identifier and the encrypted decoding information, wherein the recipient decrypts the transaction identifier and requests the decoding information using the transaction identifier, and the arbiter returns the encrypted decoding information associated with that transaction identifier to the recipient.

12. A method of operating a recipient's messaging system to assure that a message sent to a recipient was requested for opening by the recipient, the method comprising:

receiving an encrypted message that was encrypted using a session key;

receiving an encrypted transaction identifier associated with the encrypted message;

decrypting the transaction identifier;

generating a request for the encrypted session key based on the transaction identifier;

sending the request to an arbiter;

receiving the encrypted session key;

decrypting the encrypted session key to provide a decrypted session key; and

decrypting the encrypted message using the decrypted session key.

13. A method of operating a sender's messaging system to assure that a message sent to a recipient was requested for opening by the recipient, the method comprising:

encrypting a message using a session key to provide an encrypted message;

encrypting the session key to provide an encrypted session key;

generating a transaction identifier;

encrypting the transaction identifier to provide an encrypted transaction identifier;

sending the encrypted transaction identifier and the encrypted session key to an arbiter server;

sending the encrypted message and the encrypted session key to a recipient; and

receiving a notification, from the arbiter, in response to a request from the recipient for the encrypted session key based on the transaction identifier.

14. A method of operating a messaging system on an arbiter server to assure that a message sent to a recipient was requested for opening by the recipient, the method comprising:

receiving a transaction identifier and an associated encrypted session key;

receiving a request, from recipient, to send the encrypted session key to that recipient, the request comprising the transaction identifier;

returning, in response to the request, the encrypted session key associated with the transaction identifier in the request; and

generating evidence that the request to send the encrypted session key was received.

15. A recipient's messaging system comprising:

a memory to store instructions and data;

a processor to execute the instructions stored in the memory;

the memory to store:

an encrypted message that was received from a sender;

one or more instructions to decrypt an encrypted transaction identifier to provide a decrypted transaction identifier;

one or more instructions to generate a request for an encrypted session key based on the transaction identifier;

one or more instructions to send the request to an arbiter;

one or more instructions to receive the encrypted session key;

one or more instructions to decrypt the encrypted session key to provide a decrypted session key; and

one or more instructions to decrypt the encrypted message using the decrypted session key.

16. A sender's messaging comprising:

a memory to store instructions and data;

a processor to execute the instructions stored in the memory;

the memory to store:

one or more instructions to encrypt a message using a session key to provide an encrypted message;

one or more instructions to encrypt the session key to provide an encrypted session key;

one or more instructions to generate a transaction identifier;

one or more instructions to encrypt the transaction identifier to provide an encrypted transaction identifier;

one or more instructions to send the transaction identifier and the encrypted session key to an arbiter server;

one or more instructions to send the encrypted message, the encrypted transaction identifier and the encrypted session key to a recipient; and

one or more instructions to receive a notification, from the arbiter, in response to a request from the recipient for the encrypted session key based on the transaction identifier.

17. An arbiter comprising:

one or more instructions to receive a transaction identifier and an encrypted session key; and

one or more instructions to receive a request, from at least one recipient, to send the encrypted session key to that recipient, the request comprising the transaction identifier associated with that recipient.

18. The arbiter of claim 17 further comprising:

one or more instructions to return, in response to the request, the encrypted session key associated with the transaction identifier in the request.

19. The arbiter of claim 17 further comprising:

one or more instructions to generate evidence that the request to send the encrypted session key was received by matching stored transaction identifiers with the transaction identifier from the request and logging that the request was received.

20. An article of manufacture comprising a computer usable medium having computer readable program code embodied therein for assuring that a message sent to a recipient was received by the recipient, comprising instructions to:

encrypt a message using a session key to produce an encrypted message;

encrypt the session key using a public key to produce an encrypted session key;

generate a transaction identifier;

encrypt the transaction identifier to provide an encrypted transaction identifier;

send the encrypted session key and the transaction identifier to an arbiter;

send the encrypted message and the encrypted transaction identifier to a recipient;

generate a request for the encrypted session key based on the transaction identifier;

send the request to the arbiter; and

generate, by the arbiter, evidence that a request for the encrypted session key was received.

21. The article of manufacture of claim 20 further comprising instructions to notify the sender that the request was received.

22. An article of manufacture comprising a computer usable medium having computer readable program code embodied therein for operating a recipient computer system to assure a sender that a message sent to the recipient was received by the recipient, comprising instructions to:

decrypt an encrypted transaction identifier to provide a decrypted transaction identifier;

generate a request for an encrypted session key based on the transaction identifier;

send the request to an arbiter;

receive the encrypted session key;

decrypt the encrypted session key to provide a decrypted session key; and

decrypt the encrypted message using the decrypted session key.

23. An article of manufacture comprising a computer usable medium having computer readable program code embodied therein for operating a sender's computer system to assure the sender that a message sent to a recipient was received by the recipient, comprising instructions to:

encrypt a message using a session key to provide an encrypted message;

encrypt the session key to provide an encrypted session key;

generate a transaction identifier;

encrypt the transaction identifier to provide an encrypted transaction identifier;

send the encrypted transaction identifier and the encrypted session key to an arbiter server;

send the encrypted message and the encrypted session key to a recipient; and

receive a notification, from the arbiter, in response to a request from the recipient for the encrypted session key based on the transaction identifier.

24. An article of manufacture comprising a computer usable medium having computer readable program code embodied therein for operating an arbiter computer system to assure the sender that a message sent to a recipient

was received by the recipient, comprising instructions to:

receive a transaction identifier and an encrypted session key; and

receive a request, from at least one recipient, to send the encrypted session key to that recipient, the request comprising the transaction identifier associated with that recipient.

25. The article of manufacture of claim 24 further comprising one or more instructions to return, in response to the request, the encrypted session key associated with the transaction identifier in the request to the recipient.

26. The article of manufacture of claim 24 further comprising one or more instructions to generate evidence that the request to send the encrypted session key was received.